

## CLAIMS

1. A method for accessing resources on a private network via an intermediary server, said method comprising:

5 (a) receiving a login request from a user for access to the intermediary server;

(b) authenticating the user;

(c) subsequently receiving a resource request from the user at the intermediary server, the resource request requesting a particular operation  
10 with respect to a resource from the private network;

(d) obtaining access privileges for the user;

(e) determining whether the access privileges for the user permit the user to perform the particular operation at the private network; and

(f) preventing performance of the particular operation at the private  
15 network such that a response to the resource request is not had when said determining (e) determines that the access privileges for the user do not permit the user to perform the particular operation at the private network.

2. A method as recited in claim 1, wherein the particular operation is one  
20 of a resource request, a file access operation or an email operation.

3. A method as recited in claim 1, wherein said authenticating (b) determines whether the user is authenticated based on an external authentication server.

4. A method as recited in claim 3, wherein the external authentication server is within the private network.

5. A method as recited in claim 1, wherein the intermediary server stores  
30 the access privileges for a plurality of users.

6. A method as recited in claim 1, wherein the intermediary server stores an authentication identifier for each of a plurality of users, the authentication identifier identifies an external authentication server to be used to perform said authenticating (b).

5

7. A method as recited in claim 6, wherein the external authentication server is within the private network.

8. A method as recited in claim 7, wherein the authentication identifier comprises a network address for the external authentication server.

10

9. A method as recited in claim 1, wherein the resource request is from a client-side application operating on a client machine.

15

10. A method as recited in claim 9, wherein the client-side application is selected from the group consisting of a web browser, an email application or a file access application.

20

11. A method as recited in claim 1, wherein the user is a remote user.

12. A method as recited in claim 1, wherein the resource request is from a client-side application operating on a remote client machine.

13. A method as recited in claim 1, wherein the private network is an intranet or other network.

25

14. A method as recited in claim 1, wherein the resource request is from a network browser.

15. A method as recited in claim 1, wherein said method further comprises:  
(g) performing the particular operation at the private network to determine a response to the resource request when said determining (e)

30

determines that the access privileges for the user permit the user to perform the particular operation at the private network.

16. A method as recited in claim 1, wherein the user has an Internet

5 Protocol (IP) address associated therewith, and

wherein said determining (e) comprises:

(e1) determining whether the access privileges for the user permit the user to perform the particular operation at the private network; and

10 (e2) determining whether the IP address associated with the user is authorized.

17. A method as recited in claim 16, wherein said determining (e) further comprises:

15 (e3) determining whether time-of-day restrictions are satisfied.

18. A method as recited in claim 17, wherein the access privileges comprise permitted operations, authorized IP addresses, and time-of-day restrictions for a plurality of users.

20 19. A method for providing remote access to a private network via an intermediary server, said method comprising:

(a) receiving a login request from a remote user for access to the intermediary server;

25 (b) determining whether the remote user is permitted access to the intermediary server;

(c) granting the remote user access to the intermediary server when said determining (b) determines that the remote user is permitted access, the granted access also carries access privileges to predetermined portions of the private network;

30 (d) subsequently receiving a resource request from the remote user at the intermediary server, the resource request requesting a particular resource;

(e) determining whether the resource request from the remote user is permitted by the access privileges;

(f) supplying the particular resource to the remote user when said determining (e) determines that the resource request from the user is

5 permitted; and

(g) denying the remote user from access to the particular resource when said determining (e) determines that the resource request from the user is not permitted.

10 20. A method as recited in claim 19, wherein said supplying (f) comprises:

(f1) retrieving the particular resource from a content server;

(f2) modifying at least one URL within the particular resource; and

(f3) sending the modified resource to the remote user.

15 21. A method as recited in claim 19, wherein said supplying (f) comprises:

(f1) modifying the response so that links within the response point to the intermediate server; and

(f2) sending the modified resource to the remote user.

20 22. A method as recited in claim 19, wherein said supplying (f) comprises:

(f1) determining a host name for a remote server hosting the particular resource being requested;

(f2) sending a request for the particular resource to the remote server based on the determined host name; and

25 (f3) receiving, at the intermediary server, a response to the request from the remote server.

23. A method as recited in claim 22, wherein said supplying (f) comprises:

30 (f4) modifying the response so that links within the response point to the intermediate server; and

(f5) sending the modified resource to the remote user.

24. A method as recited in claim 23, wherein the private network is an intranet.

25. A method as recited in claim 23, wherein the resource request is from  
5 a network browser.

26. A method as recited in claim 23, wherein the resource request is from a client-side application operating on a remote client machine.

10 27. A method as recited in claim 25, wherein the client-side application is selected from the group consisting of: a web browser, an email application or a file access application.

28. A method as recited in claim 19, wherein the private network is an  
15 intranet or other network.

29. A method as recited in claim 19, wherein the resource request is from a network browser.

30. A method as recited in claim 19, wherein the resource request is from a client-side application operating on a remote client machine.

31. An intermediary server system, comprising:  
a web server that receives requests for resources from client machines  
25 via a network;

a protocol handler operatively connected to said web server, said protocol handler receives the requests for resources, modifies the requests to be directed to appropriate remote servers via the private network, and forwards the modified requests for resources to the appropriate remote  
30 servers; and

a content transformer operatively connected to said protocol handler, said content transformer receives the resources supplied by the appropriate remote servers in response to the modified requests and modifies the

resources such that at least certain links contained therein are modified to be directed to said intermediary server system instead of remote servers.

32. An intermediary server system as recited in claim 31, wherein said

5 intermediary server system further comprises:

an authentication manager that manages access by said client devices to resources on the private network; and

a data store for storage of session authentication information and access privileges for the users,

10 wherein access to the resources is not permitted unless the user requesting the access is authenticated and has sufficient access privileges.

33. A system as recited in claim 32,

15 wherein said system further comprises an authentication server provided within said private network for authenticating the users to provide authentication results, and

wherein said intermediary server permits or denies access to said private network via said intermediary server by the users based on the authentication results.

20

34. A computer readable medium including at least computer program code for enabling access to resources on a private network via an intermediary server, said computer readable medium comprising:

25 computer code for receiving a resource request from a user at the intermediary server, the resource request requesting a particular operation with respect to a resource from the private network;

computer code for obtaining access privileges for the user;

computer code for determining whether the access privileges for the user permit the user to perform the particular operation at the private network;

30 and

computer code for preventing performance of the particular operation at the private network such that a response to the resource request is not had when said computer code for determining determines that the access

privileges for the user do not permit the user to perform the particular operation at the private network.

35. A computer readable medium as recited in claim 34, wherein the particular operation is one of a resource request, a file access operation or an email operation.

36. A computer readable medium as recited in claim 34, wherein said computer code for authenticating determines whether the user is authenticated based on an external authentication server.

37. A computer readable medium as recited in claim 34, wherein the intermediary server stores the access privileges for a plurality of users, and wherein the intermediary server stores an authentication identifier for each of a plurality of users, the authentication identifier identifies an external authentication server to be used to perform authentication.

38. A computer readable medium as recited in claim 34, wherein the resource request is from a client-side application operating on a client machine, and wherein the client-side application is selected from the group consisting of a web browser, an email application or a file access application.

39. A computer readable medium as recited in claim 34, wherein said computer readable medium further comprises:  
computer code for performing the particular operation at the private network to determine a response to the resource request when said computer code for determining determines that the access privileges for the user permit the user to perform the particular operation at the private network.

40. A computer readable medium as recited in claim 34, wherein the user has an Internet Protocol (IP) address associated therewith, and wherein said computer code for determining comprises computer code for determining whether the access privileges for the user permit the user to

perform the particular operation at the private network, and computer code for determining whether the IP address associated with the user is authorized.

41. A computer readable medium as recited in claim 40, wherein said  
5 computer code for determining further comprises computer code for determining whether time-of-day restrictions are satisfied.

42. A computer readable medium as recited in claim 41, wherein the  
access privileges comprise permitted operations, authorized IP addresses,  
10 and time-of-day restrictions for a plurality of users.

43. A computer readable medium as recited in claim 34, wherein said  
computer readable medium further comprises:  
computer code for receiving a login request from a user for access to  
15 the intermediary server; and  
computer code for authenticating the user.

44. A computer readable medium including at least computer program  
code to facilitate access to a private network via an intermediary server, said  
20 computer readable medium comprising:

computer program code for receiving a login request from a user for  
access to the intermediary server;

computer program code for determining whether the user is permitted  
access to the intermediary server;

25 computer program code for granting the user access to the  
intermediary server when said computer program code for determining  
determines that the user is permitted access, the granted access also carries  
access privileges to predetermined portions of the private network;

30 computer program code for subsequently receiving a resource request  
from the user at the intermediary server, the resource request requesting a  
particular resource;

computer program code for determining whether the resource request  
from the user is permitted by the access privileges;



computer program code for supplying the particular resource to the user when said computer program code for determining determines that the resource request from the user is permitted; and

computer program code for denying the user from access to the particular resource when said computer program code for determining determines that the resource request from the user is not permitted.

45. A computer readable medium as recited in claim 44, wherein said computer program code for supplying comprises:

computer program code for retrieving the particular resource from a content server;

computer program code for modifying at least one URL within the particular resource; and

computer program code for sending the modified resource to the user.

46. A computer readable medium as recited in claim 44, wherein said computer program code for supplying comprises:

computer program code for modifying the response so that links within the response point to the intermediate server; and

computer program code for sending the modified resource to the user.

47. A computer readable medium as recited in claim 44, wherein said computer program code for supplying comprises:

computer program code for determining a host name for a remote server hosting the particular resource being requested;

computer program code for sending a request for the particular resource to the remote server based on the determined host name; and

computer program code for receiving, at the intermediary server, a response to the request from the remote server.

48. A computer readable medium as recited in claim 47, wherein said computer program code for supplying comprises:

computer program code for modifying the response so that links within the response point to the intermediate server; and

5 computer program code for sending the modified resource to the user.

49. A computer readable medium as recited in claim 44, wherein the resource request is from a client-side application operating on a remote client machine.

10

50. A computer readable medium as recited in claim 49, wherein the client-side application is selected from the group consisting of a web browser, an email application or a file access application.